Bibliotheca Nostra.
Śląski Kwartalnik Naukowy
nr 4 (42) 2015, s. 54-66

Andrzej Koziara
Biblioteka Uniwersytetu Śląskiego w Katowicach

Bezpieczeństwo systemów informatycznych w bibliotekach – modele pracy systemów bibliotecznych

Koniec pierwszego i pierwsza połowa drugiego dziesięciolecia XXI w. to czas gwałtownego rozwoju zastosowań mikroelektroniki w zakresie teletransmisji danych, ingerującego w postrzeganie świata przez współczesnych ludzi. Sytuacja, którą podsumował Stanisław Lem słowami: „Kto powoduje kim? Technologia nami, czy też my – nią? Czy to ona prowadzi nas, dokąd chce, choćby do zguby, czy też możemy zmusić ją do ugięcia się przed naszym dążeniem?" (2000, s. 16). We współczesnym świecie przepełnionym różnymi ofertami opisywanymi nie językiem technologii, ale marketingu, szczególną rolę odgrywa kadra inżynierska, która powinna podejmować działania oceniające, oparte na całościowej wiedzy technologicznej. Z ocenami tymi muszą się liczyć opisywani w normach PN-ISO/IEC 27001:2014-12 i PN-ISO/IEC 27002:2014-12 członkowie „najwyższego kierownictwa". Sposób przygotowania racjonalnych decyzji, opartych na niezbędnych właściwościach technologii musi być taki, by nie tworzyć sytuacji analogicznych do opisywanych przez S. Lema w *Kongresie futurologicznym*, gdzie świat ułudy przeplatał się ze światem rzeczywistym (1983). Postępowanie takie jest szczególnie ważne, gdy trzeba dokonać wyboru modelu pracy systemów dla instytucji, które na rynku informatycznym klasyfikujemy jako niszowe. Są to takie instytucje, które realizują nietypowe lub rzadko występujące na rynku usługi, lub adresują swoje usługi do odbiorców posiadających bardzo zróżnicowane potrzeby. Przy analizie implementacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w takich instytucjach zwracamy uwagę na wszystkie elementy bezpieczeństwa, nie zapominając o konieczności osiągania odpowiedniego współczynnika dostępności systemu, który powinien być dobierany tak, by jego wartość odpowiadała rzeczywistym wymaganiom zainteresowanych.

Celem przeprowadzonych badań i prezentowanego tekstu jest dostarczenie kadrze zarządzającej bibliotekami oraz właściwym do sprawowania nadzoru nad ich działalnością organom, uporządkowanych informacji dotyczących modeli pracy systemów informatycznych, wspomagających pracę instytucji. Zagadnienie to jest istotne dla uzyskania pożądanych efektów w organizacji pracy, m.in. z uwagi na fakt, iż odpowiedzialności za dobrze dobrane i wydajne narzędzia nie ponoszą służby informatyczne, lecz naczelna kadra zarządzająca. W tej sytuacji rola służb informatycznych winna ograniczać się do rzetelnej oceny wszystkich rozwiązań i dostarczenia materiału niezbędnego do podjęcia decyzji. Niestety, decyzje dotyczące rozwiązań w zakresie wspomagania zarządzania instytucją bardzo często podejmowane są pod wpływem działań marketingowych producentów i dostawców oprogramowania i usług lub są wymuszane przez organizacje będące dysponentami środków finansowych. Tylko rzetelna wiedza, którą powinni posiadać członkowie naczelnego kierownictwa, może uchronić instytucję przed mylnymi decyzjami skutkującymi wieloletnim zmniejszeniem ilości lub jakości usług przez nią świadczonych.

Przyglądając się z zewnątrz bibliotekom naukowym, należy stwierdzić, że rola, jaką wyznaczają im rozwiązania ustawowe oraz oczekiwania społeczności danego regionu, powoduje, że w sposób oczywisty kwalifikujemy je właśnie do instytucji unikalnych na danym terenie. Specyfika bibliotek naukowych poprzez świadczone przez nie usługi informacyjno-biblioteczne odróżnia je nie tylko od pozostałych bibliotek publicznych, ale również różnicuje ich zadania w zależności od uczelni, której są elementem. W takiej sytuacji, przystępując do analiz zmierzających do wypracowania w organizacji systemów informatycznego wspomagania procesów biznesowych książnic, trzeba w sposób szczególny zająć się inwentaryzacją wszystkich potrzeb ich użytkowników. Podczas prowadzenia takich analiz należy również uwzględnić fakt, że w każdej instytucji takiego typu są już eksploatowane wielorakie urządzenia technologii bibliotekarskiej. Mowa tutaj m.in.: o urządzeniach do samodzielnego wypożyczania książek, zwrotu i sortowania książek, rejestracji udostępnień w strefach wolnego dostępu, urządzeniach do przeprowadzania skontrum i innym wyposażeniu pomocniczym. Równocześnie nie bez znaczenia pozostaje fakt, że system wspomagania zarządzania biblioteką musi współpracować z wdrożonymi wcześniej systemami zabezpieczeń zbiorów oraz sposobami identyfikacji czytelników.

Obszary pracy bibliotek

Prowadząc prace studialne, należy brać pod uwagę także specyficzne rozwiązania, związane z regulaminami przygotowanymi najczęściej na potrzeby całych systemów biblioteczno-informacyjnych uczelni, gdyż właśnie do takiego traktowania bibliotek zobowiązuje nas ustawa o szkolnic-

twie wyższym. W regulaminach tych mogą znajdować się specyficzne rozwiązania, których zastosowanie może wymagać oryginalnych modeli lub konfiguracji pracy systemów wspomagających pracę bibliotek.

Pracę należy rozpocząć od wykazu funkcji, które ma realizować system biblioteczny. Funkcje te ewidencjonowane są jako suma wszystkich zidentyfikowanych dla systemów biblioteczno-informacyjnych, jakie mają być obsługiwane w ramach instalacji wybranego przez nas systemu. Należą do nich m.in.:

- funkcje związane z gromadzeniem księgozbioru (wraz z obsługą darów i wymiany międzybibliotecznej, a niekiedy również obsługą lub współpracą z wydawnictwem uczelni);
- funkcje związane z opracowaniem zbiorów (w tym obsługa kartotek wzorcowych wraz z ich automatyczną aktualizacją i synchronizacją z wzorcami – w Polsce w zasobach Centralnej Kartoteki Haseł Wzorcowych – CKHW utrzymywanej przez centrum Nukat lub jej kopii przygotowanej na potrzeby bibliotek użytkujących system Prolib zlokalizowanej w Bibliotece Uniwersytetu Śląskiego);
- funkcje udostępniania księgozbioru przez bibliotekarzy (rejestracja i rozpoznawanie czytelników np. przez różnosystemowe karty biblioteczne, rejestracja udostępnień w czytelniach wolego dostępu oraz w czytelniach księgozbiorów wydzielonych lub specjalnych);
- funkcje udostępniania lub zwrotu księgozbioru na urządzeniach automatyki bibliotecznej oraz współpraca z systemami alarmowymi bramek;
- funkcje wyszukiwania selektywnego w zbiorach biblioteki obsługiwane przez przeglądarki internetowe;
- funkcje wyszukiwania selektywnego w zbiorach biblioteki obsługiwane przez aplikacje mobilne przygotowane na różne systemy operacyjne i platformy sprzętowe;
- funkcje multiwyszukiwania w zbiorach biblioteki oraz różnych deklarowanych w sposób swobodny, zależnie od udzielonych licencji, kwalifikowanych źródłach metadanych indeksujących chronione i niechronione zasoby baz danych uruchamiane poprzez przeglądarki internetowe;
- funkcje multiwyszukiwania w zbiorach biblioteki oraz różnych deklarowanych w sposób swobodny, zależnie od udzielonych licencji kwalifikowanych źródłach metadanych indeksujących chronione i niechronione zasoby baz danych uruchamiane poprzez specjalizowane aplikacje mobilne przygotowane na różne systemy operacyjne i platformy sprzętowe;
- funkcje nawigacyjne realizowane przez aplikacje mobilne doprowadzające na podstawie wyników z multiwyszukiwarek do siedzib bibliotek (nawigacja GPS) lub w ich wnętrzach do konkretnych regałów (nawigacje wewnątrzbudynkowe);
- funkcje komunikacji z innymi systemami informatycznymi eksploatowanymi na terenie uczelni, np. systemami ERP (przynajmniej w zakresie finansowo-księgowo-magazynowo-kadrowym) oraz systemami obsługi dziekanatu;

- funkcje chronionej dystrybucji danych gromadzonych w systemie bibliotecznym poprzez bramki funkcjonalne (np. bramki Z39.50, SIP-2 lub inne pracujące jako webservice) (Koziara, Razik, Śpiechowicz, Waga, 2015).

Zinwentaryzowane funkcje, jako propozycje zawartości poszczególnych modułów, są podstawą do podejmowania prac nad wyborem modelu systemu informatycznego. Podczas jego konstruowania niezwykle ważne staje się przeanalizowanie wszelkich zidentyfikowanych realizowanych funkcji, które mogą stać się źródłem zagrożeń dla bezpiecznej pracy systemu. Należy pamiętać o tym, że każdy system informatyczny nie tylko musi być poddawany „konserwacji" zmieniającej sposób jego pracy i dostosowującej go do aktualnych przepisów prawnych, ale także powinien być rozwijany i wyposażany w nowe funkcje niezbędne do uruchamiania kolejnych usług informacyjno-bibliotecznych. Rozwój ten, przy zastosowaniu niektórych form narzędzi klienckich, może prowadzić do powstawania nowych zagrożeń dla bezpieczeństwa i należy go poddawać analizie ryzyka pod kątem zmian w Systemach Zarządzania Bezpieczeństwem Informacji.

Modele systemów informatycznych drugiej dekady XXI w.

Analizując budowę typowego współczesnego systemu informatycznego, stwierdzamy, że dominująca jest architektura opierająca się na tzw. modelu klient–serwer, w której możemy zastosować różnorodną budowę poszczególnych elementów składowych oprogramowania stosowanego tak po stronie systemu serwerowego, jak i oprogramowania stosowanego po stronie klienta. Architektura ta jest znana już praktycznie od samego początku projektowania systemów informatycznych i w sposób realny znalazła swoje implementacje w czasach, gdy terminalami dużych systemów superkomputerowych zaczęły stawać się mikrokomputery.

Na potrzeby analizy dzielimy je na kilka obszarów uwzględniających zagadnienia budowy oprogramowania i sprzętu, na którym to oprogramowanie będzie pracowało. W szczególności na każdym etapie badania rozwiązań należy uwzględnić to, że system obsługi biblioteki składać się może z bardzo dużej liczby komponentów, które mogą pracować, wykorzystując wewnętrznie:

- System zintegrowany z wewnętrznym modelem współpracy modułów. W systemie takim może występować wewnętrzna szyna integracyjna lub inny sposób współpracy modułów. Wszystkie dane są zapisywane w wielotablicowej bazie danych pracującej na serwerze głównym. W przypadku konieczności komunikacji ze światem zewnętrznym używa się najczęściej specjalnych bramek (zwanych również serwerami funkcjonalnymi), pracujących w zależności od metodyki projektowania systemu w oparciu o standaryzowane lub dedykowane protokoły komunikacyjne (standardowo lub niestandardowo szyfrowane). W celu podniesienia bezpieczeństwa pracy

należy dostarczyć zewnętrznym producentom narzędzia bibliotek programistycznych dedykowanych do komunikacji z modułami systemu zintegrowanego. Wewnętrzna szyna komunikacyjna może zostać udostępniona przez producenta systemu zintegrowanego do komunikacji z modułami zewnętrznymi, wtedy to producent systemu dostarcza dokumentację protokołów komunikacyjnych dla przygotowania w modułach zewnętrznych specjalnych wtyczek integracyjnych. W modułach zewnętrznych dopuszcza się niekiedy zapisywanie danych poza główną bazą danych lecz zaleca się wykorzystanie tego samego motoru bazy danych. Bezpieczeństwo danych realizowane jest najczęściej przez jednolicie przygotowany system archiwizacyjny (backup).

- System wielomodułowy komunikujący się poprzez zewnętrzną szynę komunikacyjną. Szyna komunikacyjna w zależności od producenta posiada zestandaryzowany lub dedykowany system protokołów komunikacyjnych wykorzystywany przez producenta lub producentów modułów do przekazywania danych pomiędzy systemami. W zależności od architektury systemu dane są przechowywane w jednej, kilku, kilkunastu lub nawet kilkudziesięciu bazach danych. Każdy z modułów powinien posiadać własny system archiwowania danych. Należy zwrócić szczególną uwagę na bezpieczne komunikowanie się poszczególnych modułów z szyną integracyjną a także na zapewniającą odpowiedni poziom bezpieczeństwa zarządzalną szynę integracyjną oraz na wdrożenie systemu kumulującego dane do jednego archiwum głównego.
- System wielomodułowy bez szyny komunikacyjnej. Każdy z modułów, a właściwie podsystemów, posiada własną bazę danych, a komunikacja pomiędzy nimi odbywa się poprzez system bramek lub bezpośrednich wtyczek do dedykowanych baz danych. Każdy z modułów musi posiadać dedykowany system archiwowania danych. Podczas projektowania systemu niezbędna jest współpraca właścicieli praw autorskich do kodów źródłowych, a obowiązkiem eksploatującego takie systemy jest zapewnienie odpowiednich zapisów w umowach wdrożeniowych umożliwiających zachowanie odpowiedniego poziomu bezpieczeństwa danych na wszystkich etapach ich powstawania. W takiej konfiguracji szczególnie ważne staje się zbudowanie specjalistycznego systemu kumulującego dane archiwalne w jednym miejscu, gdyż brak spójnego odtwarzania systemu może spowodować sprzeczności wewnętrzne danych.
- System mieszany zawierający w sobie elementy opisane powyżej. Jest to system, nad którym najtrudniej zapanować w zakresie pełnego jego bezpieczeństwa.

Projektowanie, wdrażanie i eksploatacja systemu zarządzania biblioteką

Przystępując do projektowania i wdrażania całości systemu wspomagającego pracę biblioteki, należy pamiętać, że praktycznie każdy z takich systemów jest systemem informacyjnym, więc w ich działaniu trzeba uwzględ-

niać wszystkie etapy procesów informacyjnych obejmujące generowanie, gromadzenie, przechowywanie, przetwarzanie, przesyłanie, udostępnianie, interpretację i wykorzystanie informacji. Etapy te w sposób istotny będą oddziaływać podczas projektowania całości systemu wspomagającego pracę biblioteki, a szczególną uwagę należy zwrócić na wyeliminowanie jak największej liczby barier wynikających ze sposobu udzielania licencji na wykorzystywane elementy systemu. Zgodnie z rekomendacjami do prowadzenia postępowań publicznych, przy projektowaniu nowych systemów należy zamawiać je wraz z przeniesieniem majątkowych praw autorskich do kodów źródłowych na końcowych użytkowników systemu. Licząc się z tym, że stan opisany powyżej jest idealny, w praktyce natomiast użytkownik jest niemalże zawsze niewyłącznym użytkownikiem systemów lub modułów pochodzących z różnych systemów, dla zachowania bezpieczeństwa należy zagwarantować w ramach opieki serwisowej „otwartość" systemu. Robi się to z reguły poprzez zapisy o tworzeniu przez producenta systemu bramek komunikacyjnych oraz zapewnienie możliwości korzystania z kodów źródłowych na potrzeby zmian i uzupełnień w przypadku, gdy właściciel praw majątkowych do kodów odmawia dokonywania zmian. Zasady takie należy stosować w szczególności do zakupu systemów, które mają obsługiwać w ramach licencji krajowej duże instytucje o tym samym profilu działania (np. biblioteki naukowe). Istotne dla bezpieczeństwa w zakresie licencjonowania jest takie skonstruowanie umów, by zapewniały one organizacji nieograniczony czas serwisowania oprogramowania w zakresie, który w Polityce Bezpieczeństwa Informacji, będącej elementem Systemu Zarządzania Bezpieczeństwem Informacji, został wskazany jako ważny dla zapewnienia ciągłości pracy instytucji. Dla bibliotek, składników Centrum Informacji Naukowej i Biblioteki Akademickiej w Katowicach (CINiBA), elementem tym jest m.in. stały dostęp do usług szeroko pojętego katalogu elektronicznego (przynajmniej w zakresie realizowanym w ramach OPAC i aplikacja mobilna do przeglądania zawartości zbiorów) pozwalający na odszukanie w strefie wolnego dostępu książki na półce w ramach dedykowanego jej działu[1].

W zakresie eksploatacji systemu informatycznego pierwszym zagadnieniem, którym należy się zająć jest sprawa serwerowni, gdzie zostały umieszczone fizyczne serwery oraz macierze gromadzące dane, które będzie

[1] Zagadnienie szeroko opisują m.in.: A. Białas, (2007). *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie.* Warszawa: Wydawnictwa Naukowo-Techniczne; W. Chmielarz, (2013). *Zarządzanie projektami @ rozwój systemów informatycznych zarządzania.* Warszawa: Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego; P. Fajfer, R. Pawlak, B. Swoboda, (2009). *Procesowe zarządzanie w zintegrowanych systemach informatycznych na podstawie systemu iScala.* T. 1. *Wprowadzenie teoretyczne.* Poznań: Wyższa Szkoła Logistyki; A. Januszewski, (2008). *Funkcjonalność informatycznych systemów zarządzania* T. 2. Warszawa: Wydawnictwo Naukowe PWN oraz J. Płodzień, E. Stemposz, (2005). *Analiza i projektowanie systemów informatycznych.* Warszawa: Wydawnictwo PJWSTK.

wykorzystywał system biblioteczny (nie dotyczy to serwerów przeznaczonych do innych celów niż system zarządzania biblioteką). Dla bibliotek akademickich zlokalizowanych w większych ośrodkach miejskich do wyboru są przynajmniej cztery alternatywy:

- Umieszczenie serwerów w serwerowni zlokalizowanej w bibliotece. Cechy pozytywne: możliwość doboru sprzętu i jego mocy obliczeniowej dostosowanego do rzeczywistych potrzeb, możliwość zapewnienia dedykowanej infrastruktury dostosowującej w sposób elastyczny swoje cechy dla wszystkich elementów systemu eksploatowanych w bibliotece, możliwość swobodnego dostosowanego do potrzeb biblioteki użytkowanych systemów wspomagania pracy biblioteki, pełne uniezależnienie się od stanu zewnętrznej infrastruktury sieciowej. Cechy negatywne: konieczność ponoszenia kosztów własnej infrastruktury, konieczność posiadania wykwalifikowanego personelu do utrzymania całości infrastruktury.
- Umieszczenie serwerów w serwerowni uczelni (chmura prywatna uczelni). Cechy pozytywne: brak przymusu posiadania własnej kadry do zarządzania serwerami niezbędnymi do pracy systemu bibliotecznego (nie zwalnia to od posiadania kadry zapewniającej prawidłową eksploatację innych systemów informatycznych biblioteki oraz zdalnego zarządzania systemem bibliotecznym). Cechy negatywne: z reguły brak możliwości wpływu na dobór sprzętu (wraz z jego niezawodnością) i zapewnienia odpowiedniej mocy obliczeniowej (możliwość zbyt wolnej pracy systemu), zagrożenie dostępu do systemu w przypadku awarii lub niestabilnej pracy sieci poza biblioteką, niekiedy brak wpływu na konfigurację komponentów systemu (np. silnika bazy danych), występujący często zbyt duży udział w kosztach eksploatacji serwerów, niekiedy kłopoty z komunikacją z peryferyjnymi urządzeniami technologii bibliotecznej lub np. systemami wydruku czy poczty elektronicznej.
- Umieszczenie serwerów w serwerowni miejskiej lub regionalnej (chmura prywatna regionalnego akademickiego ośrodka obliczeniowego mogąca być elementem chmury publicznej). Cechy pozytywne: identyczne jak dla serwerowni uczelni. Cechy negatywne: identycznie jak dla serwerowni uczelni z możliwością zwielokrotnienia problemów przy multiplikacji systemów w szczególności, gdy całość chmury zostaje niedoszacowana poprzez uruchamianie przez innych użytkowników (np. inne biblioteki) procesów absorbujących znaczne dynamicznie przydzielane zasoby serwerów, wysokie prawdopodobieństwo niestabilnej pracy urządzeń bibliotecznych, możliwe kłopoty w stabilnej integracji z innymi systemami pracującymi na terenie uczelni.
- Wykorzystanie chmury publicznej. Cechy pozytywne: identyczne jak dla serwerowni uczelni. Cechy negatywne: identycznie jak dla serwerowni uczelni z możliwością zwielokrotnienia problemów przy multiplikacji systemów w szczególności, gdy całość chmury zostaje niedoszacowana poprzez

uruchamianie przez innych komercyjnych użytkowników (np. inne biblioteki) procesów absorbujących znaczne dynamicznie przydzielane zasoby serwerów, wynoszenie własnych danych informacyjnych w nieznane miejsce świata – dla zasobów polskich bibliotek dotyczy to przynajmniej danych osobowych czytelników lub innych zasobów stanowiących tajemnicę organizacji ustanowioną w Polityce Bezpieczeństwa Informacji (PBI) i SZBI, bardzo wysokie prawdopodobieństwo nieprawidłowej pracy urządzeń bibliotecznych w szczególności tych, które potrzebują stabilnego łączą teleinformatycznego, bardzo wysokie prawdopodobieństwo możliwych kłopotów w stabilnej integracji z innymi systemami pracującymi na terenie uczelni (problemy stabilnych kanałów łączności – nie mylić z szybkością maksymalną transmisji).

Kolejnym elementem ważnym podczas podejmowania decyzji dotyczącej wdrożenia nowej wersji systemu, zmiany systemu lub pierwszego wdrożenia systemu pełniącego funkcję zintegrowanego systemu zarządzania biblioteką jest przeprowadzenie pełnego rozeznania ofert rynkowych. W przypadku bibliotek naukowych, gdzie systemy lub moduły wspomagające takie systemy jak już wspomniano są niszowe, należy przed podejmowaniem decyzji przeprowadzić udokumentowane rozeznanie rynku. Jest wiele aspektów, które decydują o konieczności podjęcia takich działań. Pierwszym z nich, wynikającym z prawa zamówień publicznych, jest konieczność dokonania rzetelnego rozeznania rynku z określeniem wszystkich aspektów użytkowych jakie są i będą w przyszłości ważne dla instytucji. W procesie rozeznania rynku należy pamiętać o tym, że szczególnej staranności wymagają czynności związane z pozyskiwaniem licencji na oprogramowanie, gdyż takowe wynikają ze stosowania do nich prawa autorskiego. Już na tym etapie należy definiować swoje oczekiwania związane z otwartością systemu, niezbędną do przyszłościowego integrowania kolejnych jego modułów pochodzących od tego samego lub innego dostawcy oprogramowania. Również na etapie wstępnym należy ustalać wszelkie dodatkowe warunki licencyjne związane z np. dostawą silnika bazy danych lub innych dedykowanych modułów wspomagających jego pracę.

Architektura systemu informatycznego

Następnym ważnym elementem, na który trzeba zwrócić uwagę, są szczegóły architektury samego rozwiązania informatycznego. Podczas wyboru odpowiadającego instytucji rozwiązania w szczególności należy mieć na względzie to, że zastosowane rozwiązanie techniczne powinno zapewniać bezproblemową współpracę ze wszystkimi wdrażanymi technologiami identyfikacji zbiorów i czytelników. Z wieloletnich doświadczeń architektów systemów informatycznych można wysnuć wniosek, że dla stabilnej pracy systemu obsługującego w pełnym zakresie biblioteki wchodzące w skład systemów biblioteczno-informacyjnych dużych szkół wyższych niezbędne

jest wdrażanie tzw. trójwarstwowej technologii klient–serwer. Technologia ta polega na tym, że w realnej pracy systemu występują trzy komponenty systemowe: serwer bazy danych, serwer aplikacyjny i klient serwera aplikacyjnego (Łakomy, 1995).

Realnym początkiem stosowania takich rozwiązań technologicznych była połowa lat dziewięćdziesiątych XX w., kiedy to firma Citrix, korzystając z udzielonej przez firmę licencji Microsoft na jądro systemu operacyjnego Windows Server 3.51, wprowadziła na rynek produkt serwera aplikacyjnego WinFrame 1.5, a następnie bardzo szybko WinFrame 1.6. Działanie tego produktu, bardzo innowacyjnego jak na ówczesne czasy, polegało na tym, że wszystkie programy były uruchamiane na serwerze aplikacyjnym natomiast do końcowego odbiorcy w sposób bardzo skompresowany był transmitowany obraz pulpitu, a od odbiorcy do serwera były przekazywane naciśnięcia klawiatury i ruch myszki (w chwili obecnej podobne rozwiązania są integrowane do każdego systemu operacyjnego Windows, tak w wersji serwerowej jak i stacji roboczej). Technologia ta znalazła szybkie zastosowanie w eksploatowanym przez Uniwersytet Śląski, Uniwersytet Opolski i Akademię Ekonomiczną w Katowicach systemie sieciowego rozpowszechniania baz danych InfoWare CD/HD (Koziara, 1997). Rozwiązanie to w krótkim czasie wykorzystano w Bibliotece Uniwersytetu Śląskiego do wytworzenia trójwarstwowej architektury klient–serwer dla wdrażanego właśnie systemu bibliotecznego (Koziara, 2008). Zastosowanie takiej architektury od początku jej istnienia związane było z koniecznością ograniczania ilości danych przesyłanych w sieciach rozległych. Przy jej zastosowaniu główną część transferu danych pozostawiono w serwerowniach, gdzie posadowione są serwery baz danych oraz obsługujące je serwery aplikacyjne.

W chwili obecnej trójwarstwową architekturę klient–serwer spotykamy w dwóch odmianach:

1. Systemy z usługami serwera aplikacyjnego wykorzystującego klasyczną technologię terminalową dostarczaną przez firmę Microsoft jako serwery Windows wyposażone w tzw. licencje Remote Applications lub przez firmę Citrix wraz z rozwiązaniami serwerowymi XenApp[2].
2. Systemy z usługami serwera aplikacyjnego opartego o specyfikację serwera WWW z wdrożonymi usługami komunikacji z bazą danych lub szyną integracyjną systemu.

Systemy z klasyczną technologią terminalową

Przy korzystaniu z „tradycyjnych" usług terminalowych do publikowania aplikacji dostępowych do systemu obsługi instytucji wykorzystuje się

[2] Opracowano na podstawie zawartości portali informacyjnych firm Citrix Systems, Inc. (pobrane 05 czerwca 2015, z: http://www.citrix.com) oraz Microsoft i powiązanych z nim witryn technologicznych (pobrane 05 czerwca 2015, z: http://www.microsoft.com)

dedykowany przez ich producentów program kliencki. Najczęściej podłączanie następuje bezpośrednio do publikowanych aplikacji w ramach sesji terminalowych (rzadko do „pełnego" pulpitu) poprzez protokoły Remote Desktop Protocol (RDP dla Win RmApp) lub Independent Computing Architecture (ICA dla XenApp)[3]. Wraz z wykrywaniem luk bezpieczeństwa oprogramowanie klientów jest aktualizowane wraz z całym systemem operacyjnym, co stanowi gwarancję wysokiej odporności na utratę danych. Oprogramowanie klienckie wyposażone jest w dedykowane elementy służące do sprawnego „mapowania" (wraz z jego odtwarzaniem w razie rozłączenia) tzw. portów lokalnych, (m.in. porty szeregowe, porty równoległe, porty magistral USB), do których na stacjach roboczych w bibliotekach podłącza się urządzenia dodatkowe niezbędne do prowadzenia usług bibliotecznych. Przykładowo są to zespoły elektronicznych czytników etykiet RFID, czytniki Elektronicznej Legitymacji Studenckiej czy inne czytniki wdrożonego systemu kart bibliotecznych. Do pracy z systemem zarządzania biblioteką wykorzystuje się zainstalowane na terminalach dedykowane oprogramowanie klienta przygotowane za pomocą kompilatorów dostarczanych wraz z silnikiem bazy danych. W standardowej konfiguracji transmisja pomiędzy klientem a serwerem aplikacyjnym prowadzona jest w pojedynczym kanale szyfrowanym. Można wdrożyć dodatkowe kanały szyfrujące dla elementów systemów biblioteczno-informacyjnych znajdujących się w innych lokalizacjach fizycznych.

Systemy z serwerem aplikacyjnym opartym na WWW

Zastosowanie tej wersji serwera aplikacyjnego powoduje, że jego klientem staje się zainstalowana na stacji roboczej przeglądarka internetowa. Wprowadzona zmiana, z pozoru upraszczająca konfigurację stanowiska roboczego bibliotekarza (choć dla klasycznych usług terminalowych klient RDP jest elementem systemu operacyjnego), wprowadza wiele zagrożeń związanych ze specyfiką zastosowanego narzędzia dostępowego jakim jest przeglądarka internetowa. Dzieje się tak głównie dlatego, że zostaje ona wykorzystana do celu, do którego nie zawsze jest optymalizowana. Z doświadczeń wynikających z eksploatacji systemów ERP wykorzystujących szyny integracyjne i dostęp do danych poprzez ich portal wiadomo, że dla wykorzystania dodatkowych jego funkcji najczęściej należy wprowadzać dodatkowe aplikacje dostępowe lub publikować przeglądarki internetowe w wersjach dostosowane do aktualnej wersji systemu zarzadzania firmą. Równocześnie do bezpiecznej i prawidłowej pracy z systemem zarządzania niejednokrotnie należy konfigurować przeglądarkę tak, że typowe zasoby sieci Internet nie zawsze są wyświetlane

[3] Jw.

w sposób prawidłowy. Specyfika pracy stanowisk bibliotecznych, do których podłączane są urządzenia dodatkowe, zmusza administratorów do napisania i wdrożenia dodatkowego oprogramowania sterującego tymi urządzeniami. Najczęściej oprogramowanie takie „przekształca" urządzenia technologii bibliotekarskiej w emulatory klawiatury, a dane przeczytane z takich urządzeń są przekazywane do serwera WWW tym samym strumieniem co dane pochodzące z naciskanych klawiszy. Możliwe jest także uruchamianie dodatkowego oprogramowania pracującego w tle, zapewniającego transmisję danych z urządzeń peryferyjnych do serwera WWW lub bramki transmisyjnej pracującej obok serwera WWW. Stwarza to zagrożenie mieszania się tych danych i błędów wynikających z takiego trybu pracy. Bardziej skomplikowanym procesem staje się filtrowanie danych przesyłanych z serwera WWW, które mają zostać przekazane do urządzeń technologicznych (np. podczas programowania etykiet RFID). Dane te muszą zostać wyfiltrowane z ogólnej informacji przekazanej z serwera, co najczęściej musi być wykonywane przez dedykowane pracujące w tle dodatkowe oprogramowanie uruchomione przez przeglądarkę internetową. Drugą opcją jest uruchomienie przez przeglądarkę internetową dodatkowego oprogramowania współpracującego z dedykowaną bramką pracującą przy serwerze WWW. W przypadku używania jednej przeglądarki, jako klienta systemu bibliotecznego i klienta zasobów sieci Internet dodatkowym zagrożeniem dla bezpieczeństwa stają się wszelkie szkodliwe, niewidoczne elementy publikowane na portalach informacyjnych, które ze względu na swoją oryginalność nie zostaną zidentyfikowane np. przez programy antywirusowe jako zagrożenia dla utraty lub zmiany danych. Działanie ich najczęściej polega na przekonfigurowaniu przeglądarki tak, by stała się ona źródłem rozpowszechniania danych chronionych. Jako typowe dla tego typu zagrożeń są: „tabnabing", czyli metoda ataku na modyfikacji strony WWW w przeglądarce w nieużywanej zakładce oraz „clickjacking", czyli podszywanie kodu pod „klikalne" elementy strony WWW (Cieślik, 2015). Zagrożenia te należą do grupy tych, których prawdopodobieństwo wystąpienia zmienia się wraz wersjami oprogramowania przeglądarek internetowych używanych jako klient do systemu zarządzania procesami instytucji. Poziom zagrożenia wynikający z prowadzonej analizy ryzyka[4] jest oczywiście zależny od innych czynników zapewnienia bezpieczeństwa i w większości przypadków niezbędne jest całkowite odcięcie dostępu do Internetu dla komputerów, na których używamy klienta przeglądarkowego dla systemu zarządzania. W takim przypadku szczególnie ważne staje się dostosowanie do zapisów niewprowadzonej przez Polski Komitet Normalizacyjny do polskiego ładu normy ISO/IEC

[4] Dotyczy zapisów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. (Rozporządzenie, 2012) oraz normy – (Technika informatyczna, 2014).

27018:2014 „Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors" (Cygan, 2015, s. 40).

Podsumowanie

Analizując opisywane aspekty wyboru systemu do obsługi biblioteki, trzeba zawsze pamiętać o tym, że podstawowym zadaniem systemów wspomagających procesy biznesowe jest zapewnienie „tu i teraz" prawidłowej pracy instytucji. Decyzje związane z bezpieczeństwem ciągłości dostępu do informacji podejmowane przez „naczelne kierownictwo" powinny opierać się na szczegółowej analizie ryzyka. Powinna ona być nakierowana głównie na elementy związane z wpływem nieprawidłowo działających systemów informatycznych na możliwość świadczenia usług w siedzibie instytucji. Przy sprawnie działającym systemie lokalnym dostępne współcześnie techniki integracji usług świadczonych drogą elektroniczną umożliwiają nam podłączanie kolejnych źródeł informacyjnych dla użytkowników wewnętrznych i zewnętrznych biblioteki w sposób całkowicie dla nich „przeźroczysty". Ze względu na koszty wdrożenia technologii bibliotecznych podejmowane decyzje mają wieloletnie skutki oddziaływujące na zakres i jakość świadczonych przez biblioteki usług w szczególności, gdy są podejmowane bez uwzględniania szczegółów odróżniających nas od innych form prowadzenia działalności biznesowej[5].

Bibliografia

Cieślik, A. (2015). Zapobieganie włamaniom. *IT Professional*, *48*(11), 12–17.

Cygan, T. (2015). Standaryzacja bezpieczeństwa w chmurze. Norma ISO/IEC 27018:2014. *IT Professional*, *45*(8), 40–42.

Koziara, A. (1997). System sieciowego rozpowszechniania baz danych: konsorcjum bibliotek naukowych wyższych uczelni Górnego Śląska. *Zagadnienia Informacji Naukowej, 2*, 98–106.

[5] Szczegółową informację zawierają opracowania: M. Pańkowska, S. Stanek (red.) (2013). *Wyzwania w rozwoju podstaw metodycznych projektowania systemów informatycznych zarządzania.* Katowice: Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach; F. Wołowski, J. Zawiła-Niedźwiecki (2012) *Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi.* Warszawa: Wydawnictwo Edu-Libri; S. Wrycza (1999). *Analiza i projektowanie systemów informatycznych zarządzania. Metodyki, techniki, narzędzia.* Warszawa: Wydawnictwo Naukowe PWN, a także norma (Technika informatyczna, 2014) – Information technology -- Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, (2014). Genewa z: ISO oraz rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Rozporządzenie, 2012).

Koziara, A. (2008). Rozwój systemów informatycznych wspomagających udostępnianie zbiorów własnych, elektronicznych baz danych i naukowych zasobów w sieci Internet. W: M. Kycler, D. Pawelec (red.), *Biblioteka otwarta : wczoraj i jutro Biblioteki Uniwersytetu Śląskiego* (s. 161–172). Katowice: Oficyna Wydawnicza Wacław Walasek.

Koziara, A., Razik, G., Śpiechowicz, A., Waga, M. (2015). Informatyczne wspomaganie usług biblioteki akademickiej. System zintegrowany – integracja systemów. W: *Biblioteka w społeczeństwie wiedzy. Informacja, edukacja, profesjonalizm, Łódź, 9–11 czerwca 2015 r.* Łódź: Biblioteka Uniwersytetu Łódzkiego [niepublikowane].

Lem, S. (1983). *Kongres futurologiczny* ; *Maska*. Kraków: Wydawnictwo Literackie.

Lem, S. (2000). *Summa technologiae*. Wyd. 1 w tej ed. Kraków: Wydawnictwo Literackie.

Łakomy, M. (1995). *Koncepcja aplikacji klient/serwer*. Pobrane 15 czerwca 2015, z http://www.computerworld.pl/news/296333/Koncepcja.aplikacji.klient.serwer.html

(Rozporządzenie, 2012). Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz.526 z późn. zm.).

(Technika informatyczna, 2014). Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania PN-ISO/IEC 27001:2014-12 – wersja polska. (2014). Warszawa: PKN.

Andrzej Koziara

Security of operation of IT systems in libraries - operating models of library systems

Summary

Currently provided IT and library services cannot do without implementing of IT institution support systems. Selecting the system´s architecture and its location is related with the institution´s organizational system, as well as with implemented solutions in library technology. Proper organizational and technical decisions are the basic conditions of security of provided services. The study describes technical and organizational solutions that became possible in the mid 2010´s. It outlines the strengths and drawbacks of the solutions, as well as highlights the functions of the management in the managing process of provided IT services security, related to the implemented IT systems.

Keywords: IT architecture of library systems, security risks in providing IT and library services, IT technologies in a library